YOUTH SERVICES
POLICY

Title: Access to, Security of, and Use of Information Technology Resources and Mobile/Cellular/Smartphone Devices **Next Annual Review Date:** 04/30/2016	**Type:** A. Administrative **Sub Type:** 5. Information Services **Number:** A.5.1
	Page 1 **of** 8
References: ACA Standards 4-JCF-6F-04 and 4-JCF-6F-07 (Performance-Based Standards For Juvenile Correctional Facilities), 2-7078 and 2-7079 (Juvenile Probation and Aftercare Services; YS Policy Nos. A.1.4 “Investigative Services”, A.2.17 “Employee Suspensions: Pending Investigation, Enforced Annual Leave, Pending Criminal Proceedings” A.2.48 “Driver Safety Program”, A.3.1 "Asset Management", A.3.2 “Travel”, A.3.3 "Requests for Statistical Information; Collection of Fees for Reproduction of Public Records and Statistical Reports", A.5.6 “Internet and Email Usage”, A.5.10 "Information Technology (IT) Technical Support", B.3.2 “Access to and Release of Active and Inactive Youth Records”, C.1.5 "Research" and C.1.13 "Legislative Request/Communication, Media Access and Public Information"; Louisiana Property Assistance Agency Policy No. POL 201401; PPM 11 “Data Sanitization”; OIT IT Standard 6-01 Desktop Configuration; Office of Technology Services IT-POL-1-04 “Data Sanitization” and IT-STD-1-17 “Data Sanitization-Standards and Requirements”.	
STATUS: Approved	
Approved By: *Mary L. Livers, Deputy Secretary*	**Date of Approval:** 04/30/2015

I. AUTHORITY:

Deputy Secretary of Youth Services (YS) as contained in La. R.S. 36:405. Deviation from this policy must be approved by the Deputy Secretary.

II. PURPOSE:

To establish access to and use of YS information systems, to ensure compliance with federal regulations governing privacy and security of information, to protect confidential data in the event of computer equipment or mobile electronic data device loss and/or theft, and to establish guidelines for determining the need for cellular/Smartphone devices and accountability for their use by YS employees.

Employees who hold positions that include the need for a cell phone/Smartphone device may receive a cell phone stipend [refer to Attachment A.5.1 (a)] to compensate for business-related costs incurred when using their individually-owned cell phones/Smartphones. The stipend will be considered a non-taxable fringe benefit to the employee.

III. APPLICABILITY:

Deputy Secretary, Assistant Secretary, Undersecretary, Chief of Operations, Deputy Assistant Secretary, Central Office (CO) Program Manager 4, Regional Directors, Facility Directors and Regional Managers, and all employees of YS.

Each Unit Head is responsible for ensuring that all necessary procedures are in place to comply with the provisions of this policy.

IV. DEFINITIONS:

Central Office (CO) Program Manager 4 – For the purposes of this policy, the employee assigned to the Assistant Secretary to manage and monitor specific program areas.

Central Office (CO) Property Control Manager (PCM) – For the purposes of this policy, the Administrative Program Specialist over property control for YS.

Computer Equipment – Includes computer file servers, desktop/notebook computers, data communications equipment, personal digital assistants (PDA), and Smartphone's.

Confidential Data - Includes information protected by Federal, State, and/or local statutes, regulations, YS policies, or contractual language. Managers may also designate data as "confidential". Any disclosure of confidential data must be authorized by the Deputy Secretary. For illustration purposes only, some examples of confidential data include:

- Medical records;
- Youth records and other non-public youth data;
- Social Security numbers;
- Bank account numbers and other personal financial information;
- Personnel and/or payroll records; and
- Data identified by government or YS policies to be treated as confidential, or sealed by order of a court of competent jurisdiction.

Information Systems - YS and Public Safety Services (PSS) information systems that reside on computer equipment located within PSS IT; includes hardware and software components.

Louisiana Property Assistance Agency (LPAA) - Property and fleet management for the control and disposition of all state moveable property and fleet management for the State of Louisiana.

Mobile Electronic Data Device - Any electric and/or battery operated device that can be easily transported, and that has the capability for storing, processing and/or transmitting data, including but not limited to laptops, mini hard drives, back-up hard drives, Zip Drives, Flash Drives, Personal Data Assistants (i.e. PDAs, including but not limited to, cell phones/

Smartphone's, Mi-fi's, Air-cards, Hand Held PCs), or any other mobile device designed or modified to store, process and/or transmit data.

Office of Technology Services (OTS) – Ancillary agency which functions as the centralized provider of IT support services for executive cabinet agencies of state government, and is designated as the sole authority for information technology procurement.

Property Control Managers (PCMs) – Employees who are designated by Facility Directors to handle and/or coordinate property control at the facilities.

Property Liaisons (PLs) – Employees who are designated by Regional Managers to handle and/or coordinate property control at the regional offices.

Security - Those precautions and safeguards that are used to protect the integrity of, and prohibit unauthorized access to, the data stored in the information systems.
This includes computer user-IDs and passwords, computer user access rights, information system time-out parameters, restricted office access, and locked offices.

Stipend – Cash subsidy paid to an employee for using their individually-owned cell phone.

Unauthorized Access - Ability to view, add, modify, delete, print, copy, or transmit data from an information system where the individual gaining access does not have the right or the need to know such information.

Unit Head – For the purposes of this policy, Unit Head consist of Deputy Secretary, Assistant Secretary, Undersecretary, Chief of Operations, Deputy Assistant Secretary, Facility Directors, and Regional Managers.

URAC – A Uniform Request Approval Cycle form.

YS Central Office - Offices of the Deputy Secretary, Assistant Secretary, Undersecretary, Chief of Operations, Deputy Assistant Secretary, General Counsel, Regional Directors, and their support staff.

V. POLICY:

It is the Deputy Secretary's policy to make computers available to employees to perform their job duties. Computers must be used for official business only. All other uses are strictly prohibited. Access to an employee's computer by youth in the custody or under the supervision of YS is strictly prohibited, except for instructional use at schools/libraries within the secure care facilities.

All YS employees utilizing a computer or mobile electronic data device (e.g. Laptop, Flash Drive, cell phone/Smartphone, Mi-fi, Air-card, Hand Held PC, etc.) shall be responsible for the data stored, processed and/or transmitted via that computer or device, and for following the security requirements set forth in this policy.

Pursuant to YS Policy C.2.4, personal cellular phones are considered contraband and will not be allowed on the grounds of a YS secure care facility, regardless of a stipend approval.

YS Policy No. A.2.48 contains information about the use of a “Wireless Telecommunications Device” while driving in a state owned, leased, or private vehicle that is being driven on state business. Exceptions are also included in said policy.

The information contained in YS Policy No. A.3.1 regarding the inventory of property, disposal of property and/or dismantling of property, etc. applies to IT devices, etc.

VI. PROCEDURES:

A. Assignment of Computer Equipment and Mobile Electronic Devices

Requests for computer equipment or other mobile electronic devices shall be submitted through the appropriate Unit Head to the Public Safety Services (PSS) Helpdesk at (225) 925-6233, with a copy forwarded to the Undersecretary, the CO Program Manager 4, and the Central Office (CO) Property Control Manager (PCM).

Immediate supervisor or Unit Head approval shall be based on the work needs of the employee. A "Movable Property" form, pursuant to YS Policy No. A.3.1, shall be completed and signed by the employee when the computer equipment or mobile electronic device is delivered.

The PSS Information Technology (IT) Director shall not authorize the assignment of any computer equipment or mobile electronic device without the approval of the Unit Head, CO Program Manager 4 and the Undersecretary.

B. Access to IT Systems

1. Each employee authorized to use an IT system shall be assigned a unique computer-user ID and password, and shall be given the level of access necessary to complete their job duties or functions as determined by the employee's Unit Head.

2. Each Unit Head shall provide training as to the level of need on access to and use of JETS and other information systems.

C. Use of IT Systems

1. YS and PSS IT Systems facilitate decision-making, research, and timely responses to youth needs and information requests. This includes the exchange of information between all units, including law enforcement and criminal justice agencies, while respecting the confidentiality and privacy of youth records.

2. Data from IT systems shall be used for reporting statistics and general demographic information to all employees of YS, government agencies, legislative staff, media and the general public, pursuant to YS Policy Nos. A.3.3 and C.1.13.

3. Dissemination of information shall be based on the right and need to know of the person(s) making the request, thus prohibiting unauthorized access and/or dissemination of criminal record information without authorization, pursuant to YS Policy Nos. A.3.3, B.3.2, C.1.5 and C.1.13.

4. Appropriate computer software necessary for the employee to perform their assigned job duties shall be installed on an employee's assigned computer. Personal software is strictly prohibited without the authorization of the Undersecretary/designee and the PSS IT Director, pursuant to YS Policy No. A.5.10.

5. Software from outside vendors of other governmental agencies may be installed with approval from the Undersecretary/designee and the PSS IT Director to meet an internal need or to participate in a multi-agency initiative. The use of such software must not compromise YS' computer security infrastructure.

   Any violation of policies established for the use of such software, resulting in the disclosure of classified information to unauthorized persons, injury or loss to the system, unauthorized modification or destruction of system data, or loss by theft of any computer system media, may result in disciplinary action. Software installation approvals shall be maintained on file by the PSS IT Director/designee.

6. Employees are prohibited from changing a computer's hardware or system settings, opening the computer case to remove, replace or repair components, or having computer administrator rights to their assigned computer unless authorized by the PSS IT Director

7. All computer equipment and mobile devices must conform to applicable Division of Administration, Office of Information Technology Standards. The PSS IT Director is responsible for ensuring the dissemination of applicable standards to all units.

8. Employees must report state tag numbers and be able to produce computer equipment and mobile devices when requested by the CO PCM, pursuant to YS Policy No A.3.1.

9. Employees shall not provide their passwords to anyone. PSS IT staff may request an employee's password in order to troubleshoot a problem under the employee's ID. If PSS IT staff request a password, once they are finished the employee is encouraged to change their password.

10. All computer software products used throughout YS for email, anti-virus, and the information systems, must have a registered license through PSS IT.

11. All Windows desktop/notebook computers must be configured for automatic Windows Updates.

12. A minimum of once every two (2) weeks, all employees assigned the use of a notebook or laptop computer shall ensure the equipment is turned on and attached to the network for a minimum of one (1) hour to allow anti-virus and operation system updates.

13. All Windows file servers and computers must be updated by PSS IT with the latest Windows Updates at a minimum of once per month or when Microsoft issues a security threat alert.

14. Each Unit Head shall appoint staff to coordinate with the CO Program Manager 4 and/or the Chief of Operations in developing priority lists for improvements to existing information systems, and the development and design of new information systems.

D. Protection of Confidential Data on Computer Equipment

1. Information stored on computer equipment is the property of the State of Louisiana. All information that Unit Heads determine to be critical to their operations must be saved on a regular basis to a removable computer tape, CD, external hard drive, etc., and stored in a secured area or saved to a fixed media, such as a dedicated back-up file server.

2. All desktop/notebook computers must be configured to activate the screen saver password protect feature upon a maximum of 30 minutes with no keyboard/mouse activity.

E. Protection of Confidential Data on Laptops or Electronic Data Mobile Devices

1. A laptop or other electronic data mobile device must authenticate the user before access to services on or by the device are permitted. Mobile devices must be configured to time-out after 15 minutes of inactivity and require re-authentication before access to services on or by the device will be permitted. The authentication mechanism(s) must not be disabled.

2. The encryption option must be enabled on laptop computers that transmit or store confidential information. Laptops shall be protected with antivirus software, and updated daily if supported by the device.

YS e-mail is protected with centralized anti-virus and anti-spam software through PSS IT. This protection may not apply to emails systems outside of YS.

3. The use of unprotected mobile devices to access or store “confidential data” is prohibited regardless of whether the equipment is owned or managed by PSS or YS, and shall result in disciplinary action.

F. Reporting Loss/Theft of Equipment or Data

Employees are expected to secure computer equipment when left unattended. Any lost or stolen equipment shall be reported immediately by the unit’s PCM/Property Coordinator to the Unit Head, the appropriate Regional Director, and the CO PCM.

The CO PCM shall immediately notify the CO Program Manager 4, the Undersecretary, and the PSS IT Director.

The Regional Director shall immediately report the incident to Investigative Services (IS), pursuant to YS Policy No. A.3.1.

G. Temporary Disable of Systems Access (Email/Databases):

If an employee is being investigated and placed on forced leave, the employee’s email account shall be temporarily disabled until the investigation is concluded. This includes the confiscation of an assigned laptop since the employee being investigated and on forced leave could access databases on a laptop.

It is the Unit Head’s responsibility to ensure these actions are done by immediately requesting that the appropriate IT staff temporarily disable the email account, and that the assigned laptop is taken from the employee to prevent access to databases (refer to YS Policy Nos. A.1.4 and A.2.17.

H. Termination of Access to Information Technology Resources

1. Upon an employee's end of service with YS, a “Uniform Request Approval Cycle” (URAC) form shall be completed by the Facility IT staff / Regional Manager, and forwarded to the CO Program Manager 4 for approval and to be entered into the URAC system.

   The CO Program Manager 4/designee shall be informed by the Unit Head and/or PSS HR staff of the employee's departure date.

2. Upon receipt of the URAC by PSS IT, the employee’s access to all YS computer equipment, databases and/or electronic mobile devices shall be terminated effective on the employee’s separation date noted on the URAC.

3. The Unit Head may, at any time prior to the separation date, request termination of an employee's access if the situation warrants such action.

4. Requests for termination of access shall be maintained in the appropriate Lotus Notes database.

I. Requests to surplus or dispose of assets deemed to be electronic media shall be handled through the guidelines established in YS Policy No. A.3.1.

VII. SERVICE FOR CELLULAR/SMARTPHONE DEVICES:

A. YS may provide approved employees with a state issued cellular/Smartphone device and service, following approval by the Undersecretary.

B. Requests shall be communicated to the Undersecretary/designee by the Unit Head on a case-by-case basis.

C. Cellular devices issued shall be used for YS business purposes only.

D. Employees may request that they be allowed to use their individually-owned cell phones instead of the State issued cell phone. This request shall be made on the "Cell Phone Stipend Agreement" [see Attachment A.5.1 (a)], and submitted to the Unit Head for approval. The final approval shall be given by the Deputy Secretary/designee.

E. Employees with personal cellular telephone service may be reimbursed for calls related to state business. Reimbursements shall not exceed $30 (thirty dollars) per month. Requests for reimbursement must be submitted on a travel expense claim voucher on a quarterly basis (refer to YS Policy No. A.3.2).

F. All requests for reimbursement must be submitted by the Unit Head to the Undersecretary for review and approval.

G. Approved personal cellular telephones utilized to conduct state business may be subject to search and review of the device and related data.

H. Designated CO staff shall periodically review cell phone/Smartphone billing statements, and if questionable email the Unit Head to verify with the user that the calls are of a legitimate business nature.

Previous Regulation/Policy Number: A.5.1
Previous Effective Date: 10/21/2014

Attachments/References: A.5.1 (a) Cell Phone Stipend Agreement Oct2014.doc